Regulation of Internet of Things Devices to Protect Consumers: Summary Report

UTS

accan

Regulation of Internet of Things Devices to Protect Consumers

Summary Report

David Lindsay
Genevieve Wilkinson
Evana Wright

June 2022

Regulation of Internet of Things Devices to Protect Consumers: Summary Report

Authored by **David Lindsay, Genevieve Wilkinson and Evana Wright**

Published in **2022**

This project was funded by a grant from the Australian Communications Consumer Action Network (ACCAN).

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

University of Technology Sydney
Website: www.uts.edu.au
Email: david.lindsay@uts.edu.au
Telephone: 02 9514 3761

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: 02 9288 4000

If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: https://www.communications.gov.au/what-we-do/phone/services-people-disability/accesshub/national-relay-service/service-features/national-relay-service-call-numbers

ISBN: 978-1-921974-75-5
Cover image: **Design by Nathaniel Morrison with images from Shutterstock**

This work is copyright, licensed under the Creative Commons Attribution 4.0 International Licence. You are free to cite, copy, communicate and adapt this work, so long as you attribute the authors and "**University of Technology Sydney**, supported by a grant from the Australian Communications Consumer Action Network". To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/

This work can be cited as: Lindsay, D., Wilkinson, G. & Wright, E. 2022, *Regulation of Internet of Things Devices to Protect Consumers: Summary Report*, Australian Communications Consumer Action Network, Sydney.

Table of Contents

Introduction

This is the Summary Report of the project, *Regulation of Internet of Things Devices to Protect Consumers.* It summarises the main findings and conclusions of the project. The findings and conclusions are explained in detail in the Final Project Report, which can be downloaded here.

The research project commenced in August 2020 and culminated with the release of the Final Project Report in June 2022. The report responds to the legal and policy challenges posed by Consumer Internet of Things (CIoT) devices, which are increasingly common in the homes of Australians. In doing so, it makes 42 recommendations for legal and policy reforms aimed at addressing the distinctive features of CIoT devices.

During the course of the research project, there were important policy developments in relevant areas of the law, which significantly influenced the scope of the research. The project's research and the recommendations have also taken into account valuable feedback received from stakeholders, experts and colleagues; including feedback from two well-attended roundtables, which are described in the Final Project Report.

Project Objectives

In the context of CIoT devices in the home, the overall objectives of this project were:

1. To make recommendations for legal and regulatory reform, to improve consumer security and privacy;
2. To comprehensively analyse current Australian consumer, data security and privacy laws, to identify weaknesses and gaps, with the object of producing international best practice laws and regulation;
3. To provide accessible information for consumers and consumer representatives to better understand: (a) existing consumer legal rights; and (b) practical steps for consumers to better protect their security and privacy when using CIoT devices;
4. To increase understanding of the vulnerabilities of devices currently on the market, for the benefit of consumers, consumer representative groups and other stakeholders; and
5. To produce informed commentary on, and analysis of, best practice guidelines for implementing high level principles for securing CIoT devices.

This Summary Report, together with the Final Project Report, two consumer tip sheets and academic articles, aim to fulfil these objectives.

As indicated by the objectives, the project focussed on three areas of law and regulation: cyber security, consumer protection and data privacy. While CIoT devices raise issues for other areas of the law – including, for example, contract law and competition law – these three areas were selected as they are the most important for dealing with the immediate challenges facing consumers of CIoT devices.

Scope of the Project

What is the Internet of Things (IoT)?

The Internet of Things (IoT) essentially refers to physical products with embedded software that are connected to the Internet. An important characteristic of an IoT device is that it incorporates 'sensors' which enable data to be collected, distributed and acted upon.

The connected nature of IoT devices means that data can be collected from that product and software downloaded to it. This can benefit owners of the product, for example, through seamless provision by the developer of software updates to improve the functions or security of the device. Similarly, consumers can benefit from the data collected - such as by knowing more about their own patterns of use or the performance of a device. However, there can be downsides to these capacities, which create threats to a consumer's privacy and cyber security. The distinctive features of IoT devices also challenge other areas of the law including, as addressed in this project, consumer protection law.

What is the Consumer Internet of Things (CIoT)?

CIoT devices are the subset of IoT devices addressed in this Project. CIoT devices are:

> network-connected (and network-connectable) devices and their associated services that are usually available for the consumer to purchase in retail.[1]

These devices are generally complex products, which can include hardware, software, data and service components. They include connected children's toys and baby monitors; connected safety-relevant products, such as smoke detectors and door locks; smart cameras, TVs and speakers; wearable health trackers; connected home automation and alarm systems; connected appliances (eg, washing machines and refrigerators); and smart home assistants.

This project focused on CIoT devices in the home. In doing so, it specifically excluded devices intended to be worn on the person, such as health monitors. It also generally excluded other wearables, like smart watches with the single exception of a case study on a children's smartwatch. The project also excluded devices that have a primary purpose of communicating, such as conventional smartphones, tablets, desktop computers and laptops. These products were excluded as devices such as health monitors and mobile phones raise distinct regulatory issues.

[1] European Telecommunications Standards Institute (ETSI), *Cyber Security for Consumer Internet of Things* (Technical Specification No ETSI TS 103 645 v1.1.1, February 2019) <https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf>.

Case Studies

While CIoT devices are attractive to consumers, they are often unaware of the potential downsides of the products. Consumers are also normally unaware of the nature of the complex relationships that created by their purchase with possibly multiple entities in the CIoT supply chain.

To throw light on the potential problems faced by consumers of CIoT devices, the project incorporated a number of case studies of specific CIoT devices. The devices investigated by the case studies were as follows:

- Ring Doorbell – home security system
- Roomba – robot vacuum cleaner
- Google Nest – home assistant device
- Vtech Smartwatch – children's internet connected game/camera/watch
- August Smartlock – door lock control
- Tapo Smartbulb – smart light bulb that can be controlled remotely

The case studies were conducted primarily by analysing the terms and conditions of the contracts relating to the products, together with other publicly available information.

Overall, the case studies revealed immensely complex "nests" of contractual arrangements, many of which are not readily available for consideration by consumers prior to purchase. The relationships between the agreements are not always clear and there are sometimes inconsistencies. Many of the agreements are not specifically tailored to Australian circumstances and, even where they are, there is commonly reference to foreign laws. Moreover, it is common for the agreements to provide for variation of the terms and conditions without sufficient notice to consumers, and sometimes on the basis that continued use of a device amounts to agreement to a variation.

While security policies apply to all of the devices in the case studies, there is considerable inconsistency between the policies. This level of inconsistency can contribute to consumer confusion. All of the agreements make provision for software updates; but they commonly allow for unilateral modification, often without notice to the consumer, and with continued use constituting consent to the modifications.

While there is considerable diversity in the privacy policies and standards found in the agreements, the policies commonly place most responsibility for protecting privacy on consumers. Furthermore, in general, the privacy policies are not designed specifically for Australian privacy law, and sometimes reference foreign laws, particularly the European Union General Data Protection Regulation (the 'GDPR').

Cyber Security

CIoT devices are 'always connected, always on'. This means that, unlike conventional, unconnected consumer products, they are susceptible to security breaches. At present, responsibility for securing CIoT devices is placed largely on consumers; and many consumers are not fully aware of the steps needed to properly secure their devices. The security issues associated with CIoT devices include the following:

- *Vulnerability and weak security.* CIoT devices are vulnerable because they have limited processing power, creating challenges for the processing of data necessary to ensure security. The large number of connected CIoT devices with poor security in our society creates a large potential attack surface for malicious actors. There are also specific dangers to consumers if the security of sensitive CIoT devices, such as IoT-enabled locks, temperature-control devices or children's toys, is compromised.

- *Capacity to inflict harm remotely.* The 'always connected' nature of CIoT devices enables malicious actors to cause harms, such as unauthorised access to data or adverse effects on the operation of devices, remotely.

- *Insecurity at scale: system-wide risks.* Apart from individual harms, the vulnerabilities of CIoT devices create system-wide risks of large attacks launched by networks of insecure devices. The best known of these attacks have involved the Mirai malware, which used common factory default usernames and passwords to infect CIoT devices, such as cameras and home routers, to launch distributed denial of service (DDoS) attacks.

International Initiatives

The security of CIoT devices has been the first focus of regulatory attention.

Other than technical standard-setting activities, such as those of the International Organization for Standardization (ISO), there have been few genuine international initiatives on CIoT security. In February 2022, however, the World Economic Forum (WEF), in consultation with Consumers International, the Cyber Tech Accord and I Am the Cavalry, released a *Statement of Support,* which represented a multi-stakeholder consensus on five CIoT security essentials or principles. The consensus - which arose from expert analysis of over 100 standards, specifications and guidelines - sets out the following five 'must haves':

- no universal default passwords;
- implementing a vulnerability disclosure policy;
- keeping software updated;
- securely communicating; and
- ensuring that personal data is secure

UK Initiatives

Regulation of the security of CIoT devices in Australia has been influenced by developments in the UK. A brief history of the UK process is necessary to understand the developments in Australia.

The UK first introduced a voluntary code of practice for CIoT security in October 2018. The UK Code incorporated 13 security principles, which were arranged in order of importance. The security principles can be summarized as follows:

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security sensitive data
5. Communicate securely
6. Minimise exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is protected
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

A further UK review of the voluntary CIoT security framework mapped global IoT security and privacy standards against the European Telecommunications Standards Institute (ETSI) standard for the *Cyber Security for Consumer Internet of Things: Baseline Requirements* (EN 303 645) (the 'ETSI standard'), which arguably has become a de facto global standard.

In April 2021, the UK government announced that it would introduce legislation to regulate the security of consumer connected products, such as smart speakers, smart televisions, connected doorbells and smartphones. To do this, the Product Security and Telecommunications Infrastructure Bill 2021 (the 'PS&TI Bill') was introduced in November 2021 and this Bill is expected to be enacted in 2022.

The Bill's mandatory requirements are confined to the top three obligations in the UK Code and the ETSI standard, namely:

- **Security Requirement 1:** Ban universal default passwords;
- **Security Requirement 2:** Implement a means to manage reports of security vulnerabilities; and
- **Security Requirement 3:** Provide transparency about the length of time for which a product will receive security updates.

Australian Regulation

The Australian response to securing CIoT devices began with the overarching framework of the national Cyber Security Strategy, which was first established in 2016 and replaced by an updated strategy in 2020. In December 2019, the Australian Government initiated a consultation on a voluntary draft Code of Practice for CIoT devices. Following the consultation, the government released the final version of the Code of Practice in September 2020.

The Australian Code essentially adopted the 13 principles from the UK *Code of Practice,* but restated them, with the consultation document indicating that it 'builds upon' the UK guidelines. The 13 security principles in the Australian Code of Practice can be summarised as follows:

1. No duplicated default or weak passwords
2. Implement a vulnerability disclosure policy
3. Keep software securely updated
4. Securely store credentials
5. Ensure that personal data is protected
6. Minimise exposed attack surfaces
7. Ensure communication security
8. Ensure software integrity
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

In July 2021, the then-Government commenced consultations on options for regulatory reforms and voluntary incentives to strengthen cyber security, based on a discussion paper prepared by the Department of Home Affairs. The discussion paper included options for setting cyber security expectations, increasing transparency and protecting consumer rights, including for CIoT devices. The paper reported on government qualitative research on industry uptake of the voluntary code which found that:

- Many firms are aware of the Code of Practice but found it difficult to implement the high-level principles.
- While all participants stated a commitment to strong cyber security, many had not yet implemented a vulnerability disclosure policy, which is one of the low cost, high priority elements of the Code of Practice.

- Products sold at the lower end of the market can have less reputation to protect and thus less incentive for high cyber security.

Based on this research, the discussion paper identified two options for implementing cyber security standards in Australia:

1. maintain the status quo based on the voluntary Code of Practice; or
2. introduce a mandatory product standard for smart devices.

In relation to the possible mandatory standard, the discussion paper proposed adopting ETSI EN 303 645, and mandating compliance with either the whole of the standard or, following the UK, the top three requirements. While the discussion paper pointed to challenges in implementing a mandatory code, it observed that the benefits could outweigh the costs. Subsequently, during the 2022 federal election campaign, the then Minister for Home Affairs indicated an intention to replace the voluntary code with legislation mandating minimum standards, aligned with the UK Act. At the time of writing, the new Government had yet to announce how it would progress this process.

Analysing the UK process, other overseas experiences and the Australian developments, the Final Project Report makes the following recommendations for enhancing the security of CIoT devices. The rationales supporting the recommendations are explained in detail in the Final Project Report.

Recommendation 1: *Legislation should be introduced to regulate the security of Consumer Internet of Things (CIoT) devices. The legislation should impose mandatory minimum obligations on relevant entities, namely: manufacturers, importers and distributors of CIoT devices.*

Recommendation 2: *Australia should not mandate adoption of ETSI EN 303 645 but should build on the security principles in the current Code of Practice.*

Recommendation 3: *Legislation imposing security standards should adopt a staged approach by, in the first instance, mandating the most important standards. Consideration should be given, in the first instance, to mandating the five 'must haves' identified by the World Economic Forum (WEF), namely: no universal default passwords, implementing a vulnerability disclosure policy, keeping software updated, securely communicating and ensuring that personal data is secure.*

Recommendation 4: *Legislation setting minimum security standards should, in general, follow the model adopted by the UK Product Security and Telecommunications Infrastructure Bill 2021 by imposing duties on manufacturers, importers and distributors relating to compliance with minimum standards, statements of compliance and compliance failures.*

Recommendation 5: *Legislation imposing security standards should adopt a flexible tiered system of enforcement, potentially incorporating compliance notices, stop notices and recall notices.*

Recommendation 6: *Consideration should be given to establishing a role for the newly established Cyber and Infrastructure Security Centre (CISC) in regulating the security of CIoT devices.*

Recommendation 7: *If legislation imposing mandatory standards on CIoT devices is introduced, consideration should be given to how it relates to the broader cyber security regulatory framework,*

including the regulatory regime applying to critical infrastructure assets. Ideally, cyber security regulation should be extended beyond critical infrastructure to apply across industry sectors. While the regulation of CIoT devices presents distinct policy issues, it should be harmonised with economy-wide efforts aimed at improving incentives to enhance cyber security.

Labelling for Security

The Home Affairs discussion paper also canvassed options for introducing labelling for smart devices. While it is not a panacea, product labelling can play a role in assisting consumers to distinguish between secure and insecure products.

The Home Affairs discussion paper identified the following three options:

1. Maintain the status quo of no labelling scheme;
2. Introduce a voluntary star rating labelling scheme, similar to that implemented in Singapore or Finland; or
3. Introduce a mandatory expiry date label, in accordance with a recommendation from the Cyber Security Strategy Industry Advisory Panel.

The Final Project Report includes a detailed analysis these options. It also describes the voluntary labelling schemes introduced in Singapore and Finland. Drawing on this analysis, the report makes the following recommendations.

Recommendation 8: *Over time, a mandatory security labelling scheme should be introduced as part of a comprehensive CIoT security regulatory regime. The labelling scheme must be properly resourced to ensure satisfactory testing, certification and enforcement. The scheme should be consistent, to the extent possible, with other relevant national labelling schemes.*

Recommendation 9: *Prior to the introduction of a mandatory labelling scheme, a voluntary scheme with government backing, similar to Singapore's Cybersecurity Labelling Scheme (CLS), should be introduced and properly resourced. The Australian Government's role in supporting the scheme should extend to accrediting certification bodies and enforcement. The scheme should incorporate arrangements for certification by independent third parties and should not be based on self-certification.*

Recommendation 10: *In conjunction with the introduction of a labelling scheme, government should fund a public education campaign to increase consumer awareness of both the scheme and security issues relating to CIoT devices.*

Consumer Protection

The Final Project Report analyses the fundamental challenges CIoT devices pose for consumer protection, focusing on the Australian Consumer Law (the *'ACL'*).

The *ACL* is a national, uniform law, providing consumer protection and fair trading rules across all sectors of the Australian economy. The general objectives of the *ACL* are:

- to ensure that consumers are sufficiently well-informed to benefit from and stimulate effective competition;
- to reduce the supply of unsafe goods and related services in the Australian market and ensure they are fit for the purpose for which they are sold;
- to prevent practices that are unfair;
- to meet the needs of those consumers who are most vulnerable or are at the greatest disadvantage;
- to facilitate accessible and timely redress where consumer detriment has occurred; and
- to promote proportionate, risk based enforcement.

The distinctive features of CIoT devices mean that there are gaps or uncertainties in how the *ACL* applies to protect consumers. Many of these concerns about the operation of the *ACL* in relation to CIoT devices were illustrated in the case studies included in the Final Project Report. The main challenges CIoT devices pose for consumer protection law include the following.

- *Hybrid nature of CIoT devices:* As mentioned earlier, CIoT devices incorporate hardware, software, data and service elements. Such devices usually depend upon software, which can be automatically updated. This means that functionality and the nature of the devices may be subject to significant and potentially unpredictable changes over time. This can change how the devices work for a consumer or create unexpected difficulties for consumers in using them. The complex nature of CIoT devices may even mean that it is difficult to determine what is meant by the 'product' covered by a consumer contract with a supplier.
- *Opacity of CIoT devices*: CIoT devices usually require software upgrades, particularly to ensure the security of the devices. The often complex interactions between software, data and hardware can make it difficult for consumers to know how their devices work or why the device may not be working as expected. The provision of upgrades or changes can affect the way that devices work. Consumers often have imperfect information about the nature of the product they are purchasing, about how it might be changed and about how it works now and over time.
- *'Tethered' nature of connected device:* Compared to non-IoT products, the dependence of CIoT devices on software upgrades, including security upgrades, means that consumers are in an

ongoing relationship with service providers. This confers significant power on service providers, including the ability to impair or destroy the functionality of software-dependent devices, which is known as 'bricking'.

- *Complexity of legal liability*: The complex nature of CIoT devices, and the complex nature of CIoT supply chains, means that multiple parties are involved in the supply of such devices. These parties may include manufacturers, software providers, third party app providers, cloud service providers, other third party service providers, internet service providers (ISPs) and payment facilitators. Moreover, CIoT devices are often subject to multi-layered contracts with, for example, separate contracts relating to device hardware and software services. The complexity of CIoT devices, and of their supply chains and contractual arrangements, means that it may be difficult to determine what has gone wrong with a device and which party is legally liable if something does go wrong.

- *Complexity of ownership*: The hybrid nature of CIoT devices means that the same device may be subject to different ownership regimes. In particular, while property in the hardware may pass to the consumer, the software is likely to be subject to a licensing agreement, such as an End User Licence Agreement (EULA), with ownership remaining with the software provider. This split in ownership means that, amongst other things, unlike traditional consumer appliances, the consumer depends on a long-term relationship with a software provider, and this may have implications for ongoing use of the device.

- *Obstacles to repairing devices:* As noted previously, the complex nature of CIoT devices may make it difficult to determine what has gone wrong with a device where there is a fault or defect. Furthermore, as CIoT devices are controlled by software, consumers may encounter obstacles in having devices repaired. For example, the software may be subject to a technological protection measure (TPM), such as encryption, which can inhibit or prevent repair.

- *Consumer lock-in:* The complex nature of consumer CIoT devices means that they may depend upon a number of interacting components or products. Key component providers, such as software providers, may leverage their position to ensure that consumers are locked-in to purchasing interactive elements or products, such as apps, from either the software supplier or another preferred supplier. Given the degree to which some CIoT devices generate, or depend upon, a significant amount of consumer data, software providers may also restrict the ability of consumers to port their data to other devices, which effectively locks a consumer into a particular supplier's CIoT ecosystem.

The Final Project Report presents the case for reforms of the *ACL* to address the most important challenges for consumer law. It supports current proposals for enhancing enforcement of the *ACL*, namely introducing a prohibition on failing to provide a remedy for breach of a consumer guarantee and enhanced enforcement of the unfair contract terms law. However, the report argues that the distinctive features of CIoT devices call for more fundamental reforms. The consumer guarantees in the *ACL* establish inalienable consumer rights. Given the difficulties of shoe-horning CIoT devices into the existing categories of 'goods' or 'services', the Final Project Report recommends introducing a new category of 'digital products', which would include CIoT devices. Apart from addressing the

uncertainties in applying the existing categories to CIoT devices, this would enable the introduction of new consumer guarantees that are specifically tailored to digital products, including CIoT products. Given the considerable difficulties in accessing and understanding contractual terms and conditions and other product information, which are illustrated by the case studies, the report includes recommendations for introducing obligations for greater pre-contractual disclosure of information. It also supports the development of new technology tools to assist consumers in accessing and interpreting contractual information.

CIoT products are part of a broader constellation of data-centric technologies and business practices. To address the risks posed by these practices, including the risks of consumer manipulation, the Final Project Report supports recommendations made by the ACCC for a new general prohibition of unfair trading. That said, there are difficulties in applying consumer safeguards expressed in highly general terms, such as the statutory prohibition of unconscionable conduct and the unfair contract terms law, to new technologies and practices. To improve certainty in the application of the unfair contract terms law, the report recommends introducing a black list of prohibited contractual terms and/or a grey list of presumptively unfair terms. Furthermore, to better support enforcement of the unfair contract terms law, the Final Project Report also supports the development and use of RegTech tools by the ACCC and other regulators to assist in the identification of unfair, and potentially unfair, terms and conditions in standard form consumer contracts.

Just as CIoT devices challenge other areas of consumer law, they challenge the product liability provisions of the *ACL*, which are designed to ensure the safety of consumer products. Given the uncertainty in determining what amounts to a 'safety defect' in a CIoT device, the Final Project Report recommends producing consumer guidance, especially in relation to when a security vulnerability will amount to a safety defect. The report also recommends amending the defences in the product liability regime to ensure that it applies to defects introduced after the point of sale, such as defects introduced by software updates, and improvements to how the liability regime applies to defective components of complex products. Furthermore, the report proposes expanding the liability regime for defective products to allow for recovery for intangible harms, such as data loss and invasion of privacy. Similarly, the product recall regime should be reformed by allowing for recalls where a device causes, or is likely to cause, intangible harms, such as data loss or invasion of privacy.

The full recommendations for reforming the *ACL* are as follows.

Recommendation 11: *The Australian Consumer Law (ACL) should be amended to introduce a prohibition on suppliers and manufacturers failing to provide a remedy to consumers when legally obliged to do so under the consumer guarantees, which in the event of a major failure, would be enforced by the Australian Competition and Consumer Commission (ACCC) issuing a civil penalty notice, and a civil penalty or injunction issued by a court. Consideration should be given to providing consumers with the ability to initiate actions to enforce the prohibition.*

Recommendation 12: *Further consideration should be given to how enforcement of the consumer guarantees could be improved by the introduction of alternative dispute resolution schemes, such as ombudsman schemes.*

Recommendation 13: *A new sui generis category for digital products, distinct from 'goods' and 'services', should be introduced to the ACL. The new category should include both digital content and CIoT devices. A new category is justified because digital products are sufficiently different from traditional consumer products to merit new, specifically tailored consumer guarantees. A new category would also reduce current uncertainties in determining whether elements of a CIoT device are 'goods' or 'services'. In introducing a new legislative category, care is needed in defining the category, especially in determining when elements of a complex product are sufficiently integrated so as to form part of that product.*

Recommendation 14: *In association with the introduction of a new category of digital products, a set of consumer obligations should be developed for these products. The obligations should at least include the following: any software elements, including security software, should be up to date and regularly updated; the devices should be reasonably secure from intrusions; and the elements of a hybrid device – including software, hardware, data and associated services – should be properly integrated.*

Recommendation 15: *Suppliers of digital products, including CIoT devices, should be required to ensure that clear explanations of prescribed contractual terms, including warranties, are made available to consumers before purchase. Full contractual terms and conditions should also be publicly available on supplier websites. The conditions for complying with these obligations should be specified in regulations.*

Recommendation 16: *Additional measures should be investigated for improving access to and understandability of terms and conditions for CIoT devices. Such measures could include tools to assist in locating consumer contracts that, under Recommendation 15, would be legally required to be disclosed before purchase. In addition, measures should be investigated to assist consumers in identifying and interpreting key contractual terms, including terms in complex, interconnected contracts for CIoT devices and market comparisons between supplier terms and conditions.*

Recommendation 17: *As proposed by the ACCC, a statutory prohibition of unfair trading should be introduced. The prohibition should extend to prohibiting certain predatory and manipulative conduct associated with data-driven business models. The boundaries of any prohibition must be carefully calibrated so that it is proportionate and does not extend to legitimate business practices. Like statutory unconscionability and the unfair contract terms law, the prohibition should be regarded as a general 'safety net' that forms one part of a layered regulatory regime.*

Recommendation 18: *Legislation aimed at strengthening the remedies and enforcement of the unfair contract terms law should be reintroduced. In reintroducing the legislation, consideration should be given to including a rebuttable presumption that terms found by a court to be unfair will be presumed unfair if included in a similar contract.*

Recommendation 19: *Consideration should be given to reforming the unfair contract terms law by introducing a black list of prohibited terms, a grey list of presumptively unfair terms or, preferably, a combination of both.*

Recommendation 20: *Consideration should be given to resourcing regulators, such as the ACCC, to investigate and potentially design machine learning tools to assist in the identification of unfair terms in standard form consumer contracts. If, as recommended in this Report, the unfair contract terms law were to be amended to include prescriptive lists, such tools could enhance enforcement of the law.*

Recommendation 21: *Relevant stakeholders should provide consumer guidance on what may constitute a 'safety defect' with respect to CIoT devices (or digital products more generally), including guidance on the 'reasonable expectations' of the community in relation to product security.*

Recommendation 22: *The defence set out in Section 142(a) of the ACL should be amended such that the ACL covers defects that may be introduced by the manufacturer at a point after the original supply, for example, through software updates. Such an amendment could be enacted by introducing a new sub-section under Section 142(a), such as: 'in the case of digital products – at the time at which the digital products were supplied or subsequently modified or updated by their actual manufacturer'. This drafting is contingent upon the introduction of a category of 'digital products' being introduced into the ACL, as recommended in this Report.*

Recommendation 23: *In the event that a product liability claim involves a CIoT device with components, the consumer should be able to bring an action against the ultimate supplier or manufacturer, with the burden resting with the supplier or manufacturer to reach a determination as to liability between the providers of the component parts.*

Recommendation 24: *The liability of manufacturers under Part 3-5 of the ACL should be expanded to cover liability for all loss or damage suffered by a person because of the safety defect, regardless of whether the loss or damage is tangible or intangible, and should extend to including compensation for data loss.*

Recommendation 25: *The recall provisions under Part 3-3 of the ACL should be expanded to allow for recall (both voluntary and compulsory) of consumer goods where such goods will or may cause injury to any person or otherwise cause loss or damage, regardless of whether such loss or damage is tangible or intangible. Products should be able to be recalled where they cause or are likely to cause significant intangible harms, such as data loss or invasion of privacy.*

Recommendation 26: *A mandatory information standard for CIoT devices should be established under Part 3-3 of the ACL. The information standard should contain information to be provided to consumers that extends to the security and privacy risks associated with consumer IoT devices, the availability of software updates and the measures consumers may adopt to secure their devices.*

Data Privacy

Data privacy laws, including the Australian *Privacy Act 1988* (Cth) (the *'Privacy Act'*), are primarily concerned with regulating the collection, storage, use and/or disclosure of personal information. The main objectives of data privacy laws are:

- Redressing harms that might result from privacy breaches: and
- Protecting rights, including the autonomy and human dignity of individuals.

CIoT devices present the following main challenges to data privacy laws:

- *Mass, undifferentiated data collection.* CIoT devices are characterised by a variety of sensor technologies, such as video cameras, microphones and infrared detectors. These devices may be 'always on', resulting in the possibility of continuous sensing, watching or listening to activities in the home. Even if the devices are not 'always on', however, and the sensors need to be activated, they can result in large-scale collections of data that can be linked to individuals. Once linked to an individual, this data can reveal a considerable amount about a person and can, for example, be used to build a profile for purposes such as targeted marketing or other potentially harmful practices.

- *Data matching to draw inferences.* Data collected from CIoT devices may be combined with other data, including data from other IoT sensors, in a process known as 'sensor fusion', to draw highly revelatory inferences about individuals and their behaviour. In general, the fusion of data across devices is poorly disclosed by CIoT businesses, and its potential uses are poorly understood by consumers.

- *Blurring of boundaries.* Traditionally the home has been regarded as a 'private sphere', immune from monitoring and surveillance. By facilitating near-ubiquitous data collection and monitoring, however, CIoT devices have the potential to break down boundaries between private and public, as well as boundaries between online and offline.

- *Opaque data collection.* Many CIoT devices, which can have sensors embedded in conventional household items, such as televisions, coffee machines or bathroom scales, are designed to be unobtrusive. This can result in data being collected without people being aware. Even if household members are initially aware that data is being collected, they may become inured to this over time. Moreover, visitors to a house, or some house members, will not necessarily be aware that data is being collected, or that they are effectively being monitored.

- *Difficulties in getting informed consent.* Given the extent to which CIoT devices may collect data about a person without that person knowing, it is difficult or impossible to get consent of people, such as household members and visitors to a home, for the collection of data.

- *Increased possibility of consumer manipulation.* By extending online models of the collection and use of data into the offline world, the CIoT increases the potential for commercial entities to use the data to influence or manipulate consumers.

- *System-wide erosion of privacy.* By accepting the large-scale use of devices in the home that effectively monitor behaviour in return for the convenience offered by the devices, consumers may become habituated to everyday surveillance. Through myriad intrusions, this can contribute to the system-wide erosion of privacy and user autonomy, including the sense of what amounts to a 'reasonable expectation' of privacy.

As with consumer law, the constellation of data-centric technologies and practices, of which CIoT devices form a part, demands new approaches. In summarising the extent to which CIoT devices challenge traditional data privacy law, the Office of the Victorian Information Commissioner has observed that:

> Traditional methods used to protect privacy and better inform individuals about how their personal information is collected, used and disclosed are largely incompatible or insufficient for IoT devices. New and innovative solutions that can work with devices and services that essentially form infrastructure may be needed.[2]

Data privacy law faces particular challenges in regulating the collection, processing and use of data at scale. These issues form a key part of the current fundamental review of the *Privacy Act,* which saw the release of a major *Discussion Paper* by the Attorney-General's Department ('AGDP') in October 2021. As the issues addressed in the AGDP go beyond those raised by CIoT devices, the Final Project Report focuses on only those that are most relevant to the regulation of these devices.

In the context of the AGDP, the Final Project Report recommends adopting a completely new paradigm for data privacy regulation. This new paradigm would involve: ex ante measures, such as targeted privacy impact assessments; better calibrating protection in accordance with the risks of data technologies and practices; and ex post measures, such as targeted monitoring and auditing. The principles of privacy protection by default and by design are essential elements of this proposed new paradigm; in implementing these principles, the report recommends that lessons should be learnt from problems encountered with applying these important principles under European Union law (the GDPR). While the report overall supports a risk-based approach to data privacy regulation, it cautions that, due to inherent limitations in this approach, care must be taken in how it is applied in practice.

Addressing some of the key issues raised by the AGDP from the perspective of consumers of CIoT devices, the Final Project Report supports proposals for expanding the definition of 'personal information' and tightening the 'notice and consent' provisions. However, within this context, it is important to bear in mind the significant limitations of the 'privacy self-management' model, which

[2] Office of the Victorian Information Commissioner (OVIC), *The Internet of Things and Privacy: Issues and Challenges* (Issues Paper, February 2020) 11 <https://ovic.vic.gov.au/privacy/internet-of-things-and-privacy-issues-and-challenges/>.

underpins traditional data privacy laws but falls down in practice. Strengthened 'notice and consent' provisions must therefore be accompanied by measures designed to minimise information and consent fatigue, such as layered notices and standardised consents.

As a further response to the limitations of 'privacy self-management', the Final Project Report supports proposals for introducing a new privacy principle, requiring the collection, use or disclosure of personal information to be 'fair and reasonable'. When accompanied by an appropriate list of statutory factors, this broad principle has some potential to establish proportionate limits on new data-centric technologies and practices, including those involving CIoT devices. For example, the principle could be applied to difficult factual circumstances, such as CIoT devices that collect and process third party data without their consent. However, given that CIoT devices installed in the home are acknowledged to be 'high risk', the Final Project Report considers that there is a case for additional safeguards over and above the proposed new 'fair and reasonable' standard. In particular, the report recommends that in a specific application of the principle of privacy by default, where data processing is not essential for the functioning and security of devices, default settings for data processing by CIoT devices installed in the home should be pre-selected to 'off'. In addition, acknowledging the importance of device security for protecting consumer privacy, the report supports recommendations for improving the data security principle in Australian Privacy Principle 11 (APP 11) by clarifying what amounts to 'reasonable steps' to secure personal information.

The Final Project Report includes the following recommendations for reforming the Privacy Act.

Recommendation 27: *Australian data privacy law should be reformed to better reflect a new paradigm for regulating ubiquitous collection and processing of data that has been emerging from instruments, such as the European Union's General Data Protection Regulation (GDPR) and the European Commission's proposal for a Regulation on Artificial Intelligence. Recognising the difficulties of regulating at scale, measures should be introduced that better calibrate regulation to reflect the risks of near-ubiquitous data processing practices, while allowing for more effective regulatory oversight. Such measures could include targeted privacy impact statements, data protection by default and by design, and targeted monitoring and auditing.*

Recommendation 28: *The principle of privacy by design is an essential element of the new regulatory paradigm and should be codified as a distinct privacy principle. However, in codifying the principle, lessons should be learnt from flawed attempts to implement the principle in data privacy laws, such as the GDPR.*

Recommendation 29: *The principle of privacy by default is an essential element of the new regulatory paradigm and should be codified as a distinct privacy principle. However, in codifying the principle, consideration should be given to how the principle applies in particular contexts, with a case for stricter application of the principle to high risk acts and practices.*

Recommendation 30: *Risk-based regulation is an essential element of the new regulatory paradigm and it should be more expressly incorporated into the design of the Privacy Act. For example, the Act could distinguish between acts and practices that pose unacceptable risks, high risks or low risks.*

However, in implementing this approach, it is important to take into account the significant limitations of and problems with risk-based approaches.

Recommendation 31: *As proposed by the recent Privacy Act Review Discussion Paper produced by the Attorney-General's Department (the AGDP), the definition of 'personal information' in the Privacy Act should be amended so that it more closely aligns with the approaches taken in comparable jurisdictions and, in particular, the definition of 'personal data' under the GDPR.*

Recommendation 32: *The amendments proposed by the AGDP to support the recommended new definition, including a non-exhaustive list of the types of personal information, a list of factors to determine when a person is 'reasonably identifiable', and an amended definition of 'collection' that covers inferred information, should also be introduced.*

Recommendation 33: *Resources should be allocated to an appropriate body, such as the Office of the Australian Information Commissioner (OAIC), to investigate the potential for risk-based approaches, including a risk-based approach to defining the scope of the Privacy Act, addressing the problems of regulating data collection and processing at scale.*

Recommendation 34: *The notice provisions of the Privacy Act should be strengthened. Notice should be concise, transparent, intelligible and easily accessible, and it should clearly set out how an Australian Privacy Principles (APP) entity collects, uses and discloses personal information. Resources should be expended on ensuring that user-friendly ways of presenting notices are adopted, such as layered notices and/or standardised icons. This should be based on rigorous consumer testing.*

Recommendation 35: *The consent provisions of the Privacy Act should be strengthened. Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed, and any settings for additional data should be preselected to 'off'. Measures should be introduced to minimise consent fatigue, such as the use of standardised icons or phrases, which should be based on rigorous consumer testing.*

Recommendation 36: *As proposed in the AGDP, a new privacy principle should be introduced requiring the collection, use or disclosure of personal information to be fair and reasonable. This principle should operate in addition to other principles that apply to the collection, use or disclosure of personal information, and, in the event of inconsistencies, should prevail. As further proposed in the AGDP, the principle should be supplemented by a list of non-exhaustive statutory factors. Consideration should be given to whether the statutory factors proposed in the AGDP could be improved, such as by ensuring that a more objective standard is applied in assessing the risk of data processing.*

Recommendation 37: *Except where data processing is essential for the security and functionality of CIoT devices, default settings allowing for data processing by means of such devices should be pre-selected to 'off'.*

Recommendation 38: *As recommended by the AGDP, APP 11 should be amended to clarify what amounts to 'reasonable steps' to secure personal information, including by expressly providing that*

such steps include technical and organisational measures and a list of factors indicating what reasonable steps may be required.

Overall Themes: Future Directions

Apart from the recommendations for reforming the three specific areas of law and regulation addressed by the project, the Final Project Report identified three overall themes emerging from the research, which are areas that merit further research attention. These three areas are:

1. The challenge of aligning laws and 'joining up' regulation
2. Improving consumer education
3. Enhancing accessibility and inclusivity for vulnerable groups.

Transformative technologies, such as CIoT, can disrupt laws, resulting in laws and regulations that overlap, are inconsistent or misaligned. This is illustrated by the analysis of the laws undertaken in this project. One reason for this is that laws and law reform processes are based on pre-existing legal and policy paradigms, which each have their own rationales and are challenged by new and emerging technologies. The Final Project Report contends that a comprehensive and consistent approach is required to respond to the challenges of CIoT devices. This means ensuring that applicable laws are properly aligned.

One area that illustrates the importance of aligning laws and regulation is the potential application of multiple regimes to ensuring the security of CIoT devices. For example, the Final Project Report makes the case for introducing legislation mandating minimum security standards for CIoT devices; and it seems likely that this will occur. Meanwhile, the data security principle in APP 11 of the *Privacy Act* requires relevant entities that hold personal information to take 'reasonable steps' to secure that information. However, the current Privacy Act reform process is not considering how to align APP 11 with other laws or standards, such as mandatory security standards for CIoT devices. Furthermore, the Final Project Report explains the considerable uncertainties in how the existing consumer guarantees under the *ACL* may apply to security vulnerabilities or defects in CIoT devices. Given the importance of securing devices for consumers, the report proposes introducing a new guarantee that would require digital products to be reasonably secure. Given the potential for overlaps and inconsistencies, the report recommends further research on how best to align laws and regulations that apply to CIoT devices.

While aligning laws is important, the Final Project Report also points out that it is important to promote greater consistency between regulatory practices, which is sometimes known as 'joined-up' regulation. The need for 'joined-up' regulation arises from differences in available remedies and enforcement, but also from differences in the skills and perspectives of regulators, and differences in regulatory cultures. For example, in consultations undertaken for this project, understandable questions were raised about the appropriateness and capacity for consumer protection regulators to regulate technical issues relating to cyber security. The difficulty in allocating regulatory

responsibility for the security of CIoT devices suggests that there is a gap in the regulatory framework. To address the need for greater regulatory and policy consistency, the Final Project Report supports the establishment of a dedicated, multi-disciplinary expert body that proactively investigates the social and legal implications of transformative, or potentially transformative, technologies.

The Final Project Report emphasises that reforming laws alone is not sufficient to address the challenges and risks of the proliferation of CIoT devices. What is needed is a whole-of-society approach. Empowering consumers by, for example, building greater understanding of the promises and risks of CIoT devices is an essential element of any strategy aimed at minimising potential harms. The report therefore supports resourcing a public education to assist consumers in managing the risks posed by the devices.

While focusing on recommendations for general law reform, the Final Project Report acknowledges the particular complexities involved in balancing the undoubted benefits promised by CIoT devices for vulnerable groups and the equally important risks posed for those groups. The report points out that the best approach to addressing these complexities is to build accessibility and inclusivity into the design of CIoT devices. Moreover, any law reforms specifically aimed at supporting vulnerable groups must be accompanied by whole-of-society measures, including education of manufacturers and suppliers. Given the complexities of the specific issues faced by vulnerable groups, the Final Project Report concludes by recommending further research on how to improve accessibility and inclusivity of CIoT devices for vulnerable groups.

The Final Project Report makes the following recommendations relating to the overall themes identified in the research project and future directions for research and law reform.

Recommendation 39: *Given the extent to which CIoT devices pose fundamental legal and regulatory challenges, they should be subject to a public policy law reform process, potentially as extensive as the ACCC process investigating the regulation of digital platforms. As part of this process, further research is needed on how best to ensure that all applicable laws and regulations are aligned, including by minimising unnecessary gaps, overlaps or inconsistencies. This process could extend beyond CIoT to include the legal and policy implications of other IoT implementations.*

Recommendation 40: *Consideration should be given to establishing a dedicated, multi-disciplinary expert body that proactively investigates the social and legal implications of powerful new technologies. While not directly responsible for regulating, such a body could investigate or apply forward-looking practices such as horizon scanning, promoting the appropriate use of RegTech, and aligning applicable laws and technical standards. Consultation with diverse stakeholders, including consumer representatives and representatives of vulnerable groups, would be an important part of this work.*

Recommendation 41: *As part of a whole-of-society approach to addressing the risks posed by CIoT devices, a public education campaign should be resourced to assist consumers with managing these risks. If the recommendation for establishing the new advisory body is accepted, this body could play a role in consumer education.*

Recommendation 42: *Further research is needed on how to promote accessibility and inclusivity in relation to CIoT devices to promote the interests of vulnerable groups. This should include research on establishing a framework for promoting inclusive design of CIoT devices. Any public policy law reform process established to comprehensively address the issues raised by CIoT devices should incorporate a distinct component that investigates how to maximise the benefits and minimise the harms posed for vulnerable groups by CIoT devices.*

Regulation of Internet of Things Devices to Protect Consumers: Summary Report